# Collaborative Approaches for Medical Device and Healthcare Cybersecurity

October 21-22, 2014

Arlington, VA

# Key Note Speaker

## Marty Edwards
## Assistant Deputy Director, National Cybersecurity and Communications Integration Center (NCCIC) and Director Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

## October 21, 2014

# Session I

# Envisioning Collaboration for Medical Device and Healthcare Cybersecurity

Moderator
William Maisel, MD, MPH – Food and Drug Administration

October 21, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Key Note Speaker

## Edward J. Gabriel, MPA, EMT-P, CEM, CBCP
## Principal Deputy, Assistant Secretary of Preparedness and Response (ASPR)

## October 21, 2014

# Session II

# Cyberthreat Landscape – Framing the Problem

Moderator

Steven Curren, MS – Assistant Secretary for Preparedness and Response (ASPR)

October 21, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Session III

# Cybersecurity Gaps and Challenges: Need to Share vs. Need to Secure

Moderator
Julian Goldman, MD – Partners Healthcare System

October 21, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Session IV

# Cybersecurity Gaps and Challenges: Legacy Devices

Moderator
Kevin Fu, PhD – University of Michigan

October 21, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Session V

# Cybersecurity Gaps and Challenges: Forward Looking Design

Moderator

Thaddeus Flood, JD – Medical Imaging and Technology Association (MITA)

October 21, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Session VI

# Overview of the NIST "Framework for Improving Critical Infrastructure Cybersecurity"

Speaker
Kevin Stine, Manager of the Security Outreach & Integration Group
National Institute of Standards and Technology (NIST)

Moderator
CDR Nikhil Thakur - FDA

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Framework for Improving Critical Infrastructure Cybersecurity

## Overview and Update

**Collaborative Approaches to Medical Device & Healthcare Cybersecurity**

**October 21, 2014**

**Kevin Stine**
**Kevin.Stine@nist.gov**

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

# National Institute of Standards and Technology (NIST)

## About NIST

- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
  - 3,000 employees
  - 2,700 guest researchers
  - 1,300 field staff in partner organizations
  - Two main locations: Gaithersburg, MD and Boulder, CO

## NIST Priority Research Areas


Advanced Manufacturing


IT and Cybersecurity


Healthcare

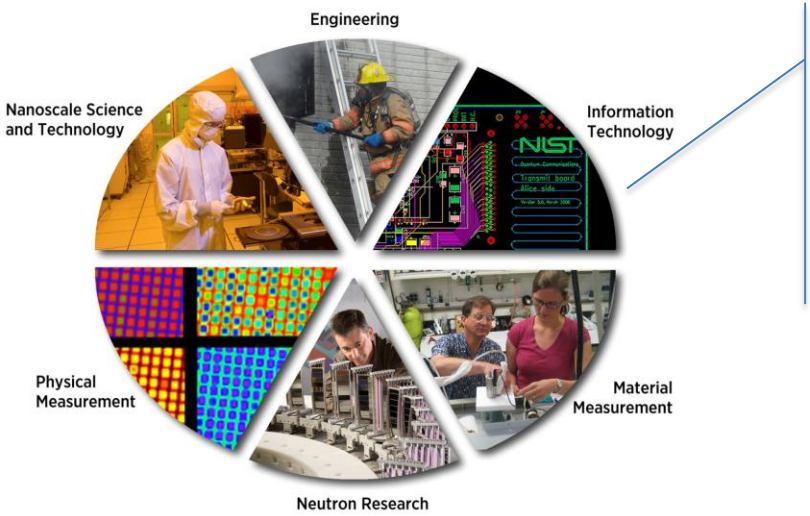

Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

# Computer Security Division




The Computer Security Division provides standards and guidelines, tools, metrics, and practices to protect information and information systems.

Biometrics – Software Assurance – Domain Name Security – Identity Management – FISMA – Security Automation – National Vulnerability Database – Configuration Checklists – Digital Signatures – Risk Management – Authentication – IPv6 Security Profile – Supply Chain – NICE – Health IT Security – Key Management – Secure Hash – PKI – Privacy Engineering– Smart Grid – Continuous Monitoring – Small Business Outreach – Mobile Devices – Standards – Cloud Computing – Usability – NSTIC – Passwords – Hardware Security – Electronic Voting – Wireless – Security Awareness – Vulnerability Measurement – Security Metrics – Public Safety Communications

# Executive Order: Improving Critical Infrastructure Cybersecurity

*"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"*

*President Barack Obama*

Executive Order 13636, *Feb. 12, 2013*

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

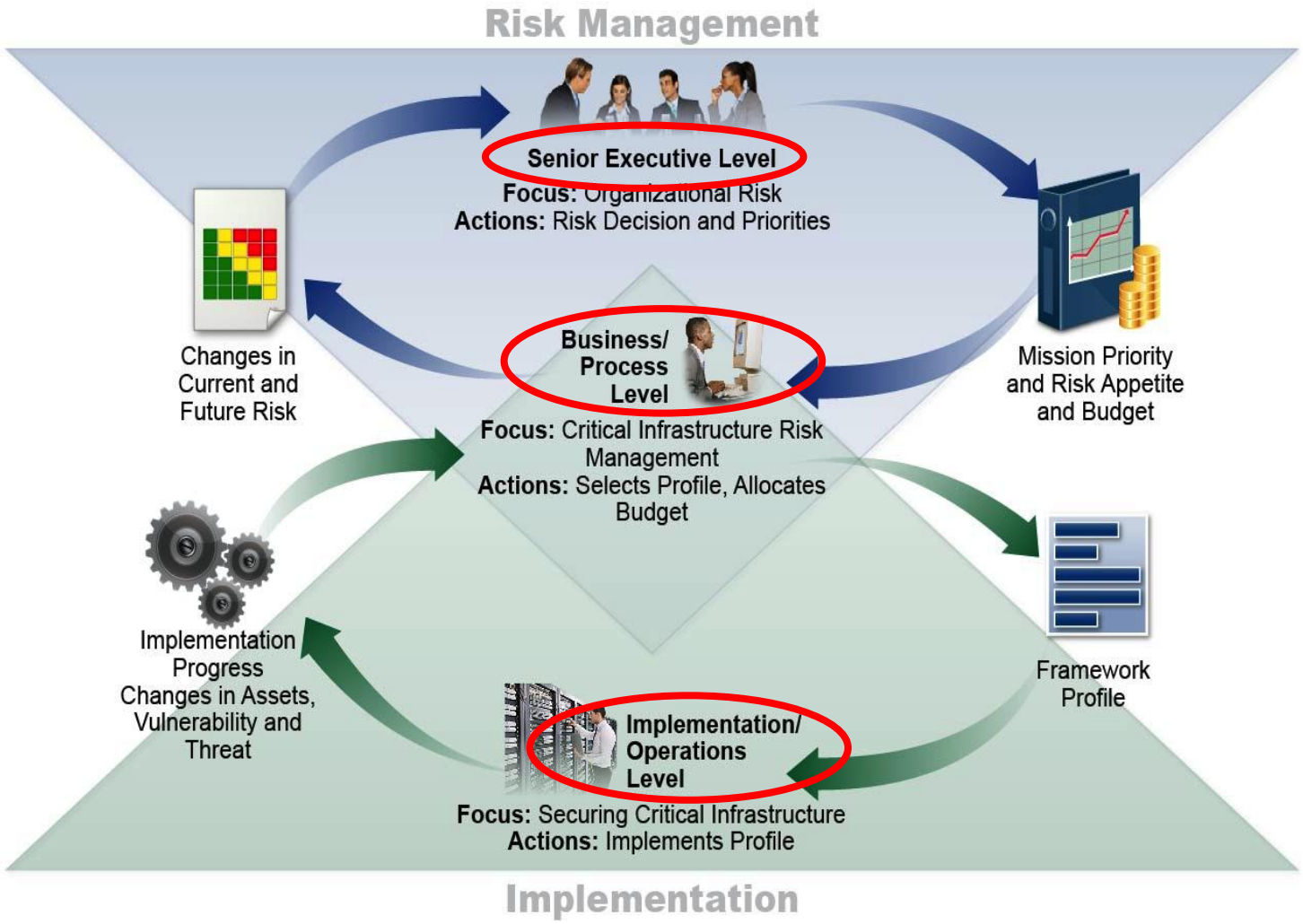
# Based on the Executive Order, the Cybersecurity Framework Must...

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations

# The Cybersecurity Framework Is for Organizations…

- Of any size, in any sector in the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don't yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

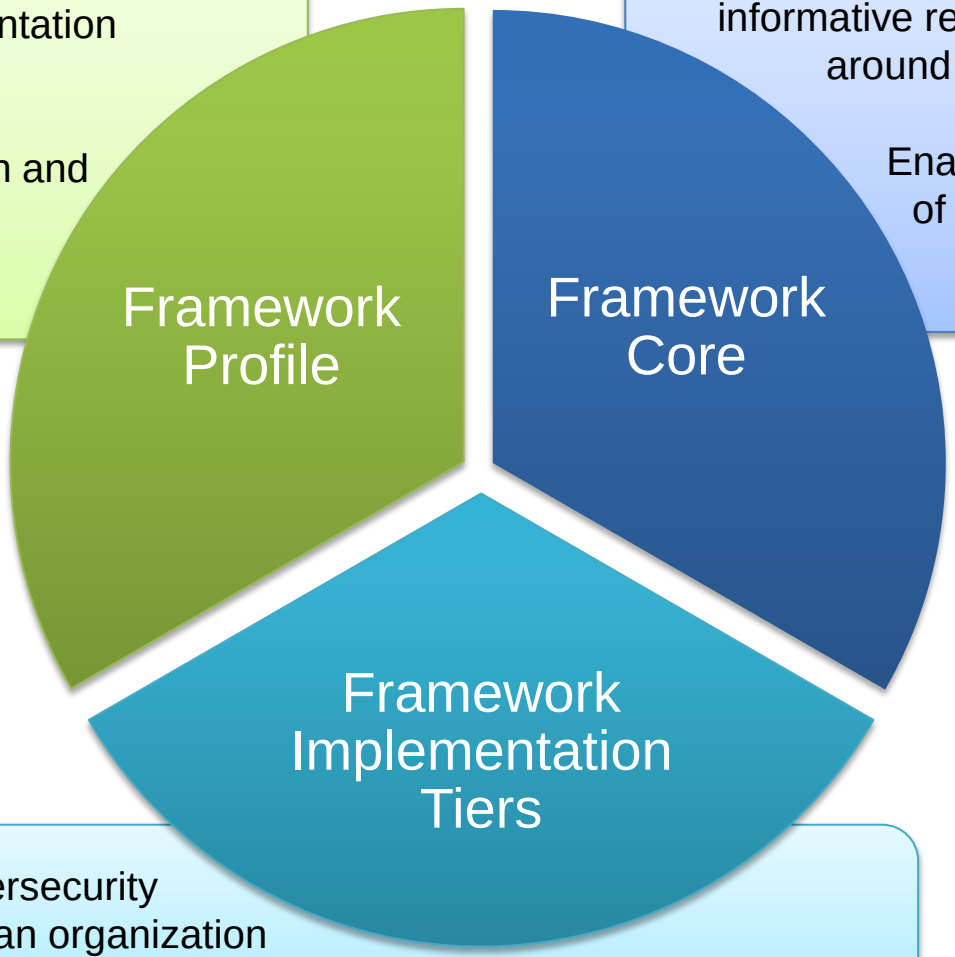
# The Framework must apply from Executives to Operations



# Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs




Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

# Framework Core

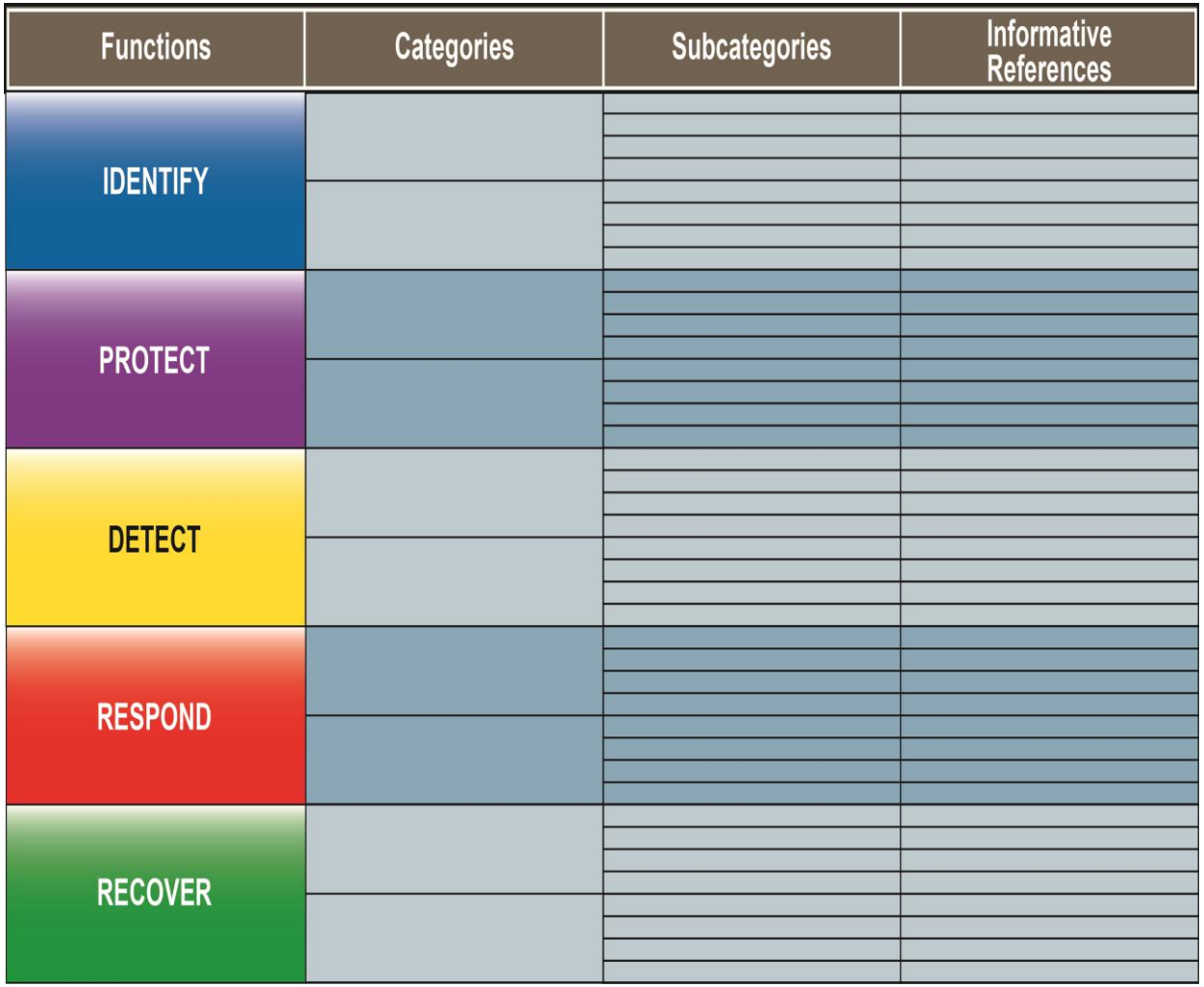
What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



# What's Next: Using the Cybersecurity Framework

- Organizations—led by their senior executives—should use the framework now, and provide feedback to NIST

- Industry groups, associations, and non-profits are playing key roles in assisting their members to understand and use the framework by:
  - Building or mapping their sector's specific standards, guidelines, and best practices to the framework
  - Developing and sharing examples of how organizations are using the framework

# What's Next: Areas for Development, Alignment, and Collaboration

- The Executive Order calls for the framework to "*identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations*"
- High-priority areas for development, alignment, and collaboration were identified based on stakeholder input:
  - Authentication
  - Automated Indicator Sharing
  - Conformity Assessment
  - Cybersecurity Workforce
  - Data Analytics
  - Federal Agency Cybersecurity Alignment
  - International Aspects, Impacts, and Alignment
  - Supply Chain Risk Management
  - Technical Privacy Standards

# Looking Forward: Current Status and Next Steps

- Framework is being used in a variety of ways
  - A recent Request for Information (RFI) on Experiences with the Framework (closed October 10th) yielded nearly 60 responses.
  - Responses are publicly available to continue an open dialogue.
    - http://www.nist.gov/cyberframework
- Workshop on October 29th-30th in Tampa, FL
  - Hosted by the Florida Center for Cybersecurity at the University of South Florida
- Roadmap items continue to be a priority

# Where to Learn More and Engage

- *Framework for Improving Critical Infrastructure Cybersecurity*, available at www.nist.gov/cyberframework
  - Share your Framework experiences at cyberframework@nist.gov
- Participate in our cybersecurity workshops and comment on our standards and guidelines
- Follow our cybersecurity activities at http://csrc.nist.gov

# Day 1 Wrap-Up
# Collaborative Approaches for Medical Device and Healthcare Cybersecurity

October 21, 2014
Arlington, VA

# Key Note Speaker

## Michael Daniel, MS, MPP
## Special Assistant to the President and
## Cybersecurity Coordinator
## White House

## October 22, 2014

# Session VII

# Adapting and Implementing the NIST "Framework for Improving Critical Infrastructure Cybersecurity"

Moderator

Deborah Kobza, CGEIT, JIEM – National Healthcare Information Sharing and Analysis Center (NH-ISAC)

October 22, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# C3 VOLUNTARY PROGRAM

OCTOBER 22, 2014

Welcome to the community.

# C³ VOLUNTARY PROGRAM OVERVIEW

"Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity."

- White House Executive Order 13636

Directives in Executive Order 13636:

- The National Institute of Standards and Technology (NIST) should develop a ***Cybersecurity Framework*** (the Framework) for reducing cyber risks to critical infrastructure
- A ***voluntary program*** for critical infrastructure cybersecurity should promote use of the Framework to help organizations improve their cybersecurity

# WHAT IS THE CRITICAL INFRASTRUCTURE CYBER *COMMUNITY*?

- Community of interest around managing cyber risk
- Builds on years of our experience partnering with industry
  - Previous industry collaborations: risk assessments for IT, Emergency Services, National Public Safety Broadband Network, and many others
- Place for industry, State and local governments, and many other organizations to identify cyber risk management needs and solutions

Goal: Transform Increased Interest → Increased Action

# SUSTAINED ENGAGEMENT

Three webinars reached more than 150 state-level officials and 100 local government officials across

**46**

states

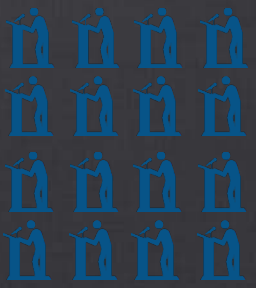
Over

**145**

Industry briefings conducted by DHS since November 2013

**16**

CISR sectors



## NEW C³VP INITIATIVES

- Partner recognition plan, including collaboration with the C³ Voluntary Program on events and outreach

# FRAMEWORK PLANNING SUPPORT

1. *Prioritize Cyber Risks*

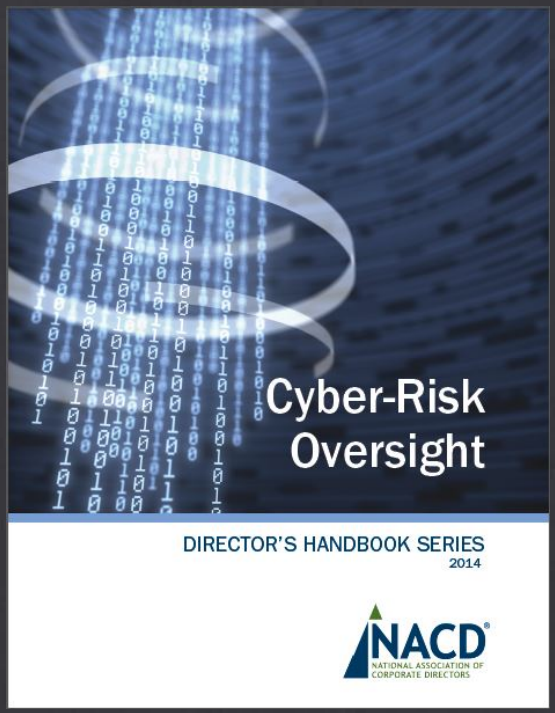
2. *Assist SSAs and industry with the development/promotion of Framework Guidance*

3. *Inform industry, sector risk management strategies*

# WEB RESOURCES


- Over **30** unique offerings are currently featured, including the **Cyber Resilience Review (CRR)** tool

- The National Association for Corporate Directors (NACD) **Handbook on Cyber Risk Oversight** is the first private sector resource



# EVENTS

- October 13: San Diego, CA
  - Part of National Cyber Security Awareness Month
  - Focus on academia, SLTT, SMBs
- October 21-22: Washington, DC (Healthcare and Public Health)
- November 10: Houston, TX (Energy)
  - Focus on Energy Sector topics
- 2015: TBA

# HOW TO GET INVOLVED

- Take advantage of C³ Voluntary Program resources
  - Visit the C³ Voluntary Program website at **www.us-cert.gov/ccubedvp**
  - Familiarize yourself with the Cybersecurity Framework
  - Download the Cyber Resilience Review (CRR) or contact DHS for an on-site assessment
  - Spread the word across your community
  - Connect with the C³ Voluntary Program about becoming a partner organization

dhs.gov/ccubedvp

# #ccubedvp

# Session VIII

# Adapting the Vision for Information Sharing and Shared Risk Assessment: Implementation within the Healthcare and Public Health Sector

Moderator
Margie Zuk, MS – The MITRE Corporation

October 22, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Key Note Speaker

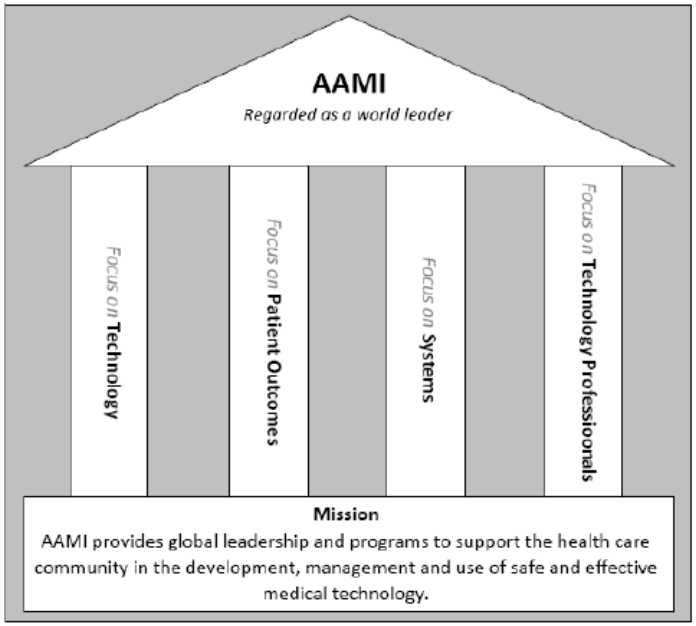

## Mary Logan, JD, CAE
## CEO & President
## Association for the Advancement of Medical Instrumentation (AAMI)


## October 21, 2014

**Mission:** Support health care community in development, management and use of safe and effective medical technology.

**AAMI's best role:** convening diverse groups to solve problems

**Best Known for:** **honest broker**




© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

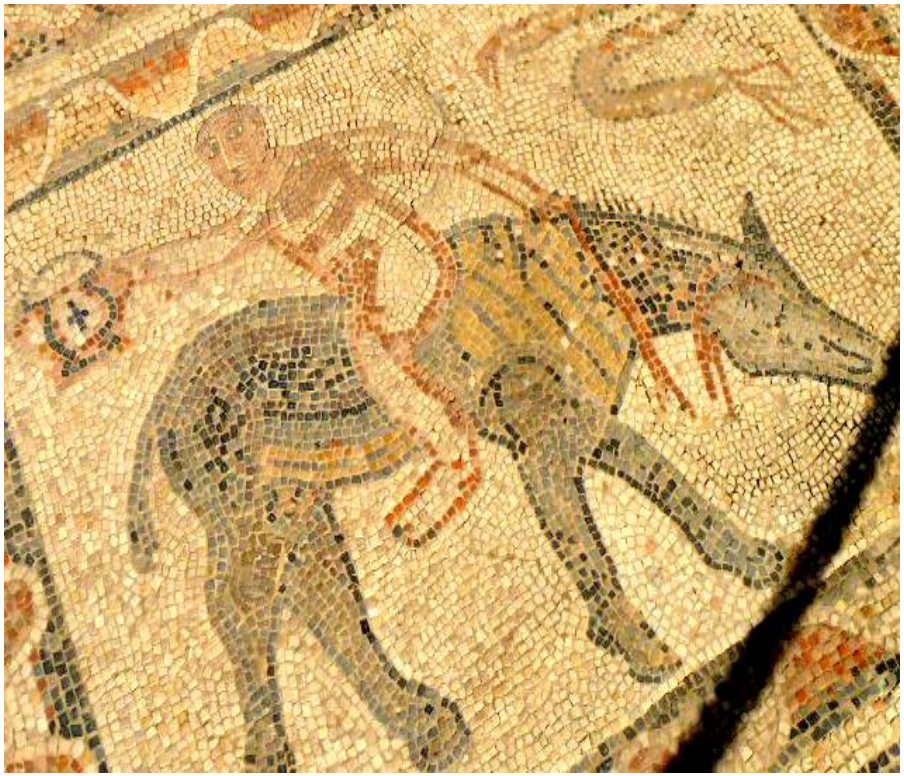
# Challenge: Technology Overload

- No design standardization
- No HDO standardization
- HDOs use old and varied products
- Proprietary features
- Not enough HF
- **Improvements – one hospital at a time**

© 2014Association for the Advancement of Medical Instrumentation www.aami.org

# Medical Device Risk: Traditional View

- FMEA
- “Normal” use
- Device-by-device
- **Healthcare not viewed as a complex, hazardous sociotechnical system**



© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

# Why We Have to Look at Risk Differently: Integration

- Dispersed regulatory scheme
- Lack of training
- No integrator
- Yet everything is being integrated


© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

# Why We Have to Look at Risk Differently: Culture

- "If you've seen one hospital, you've seen one hospital"
- Rescue model
- Authority
- Many brands, models, eras of devices used in same hospital

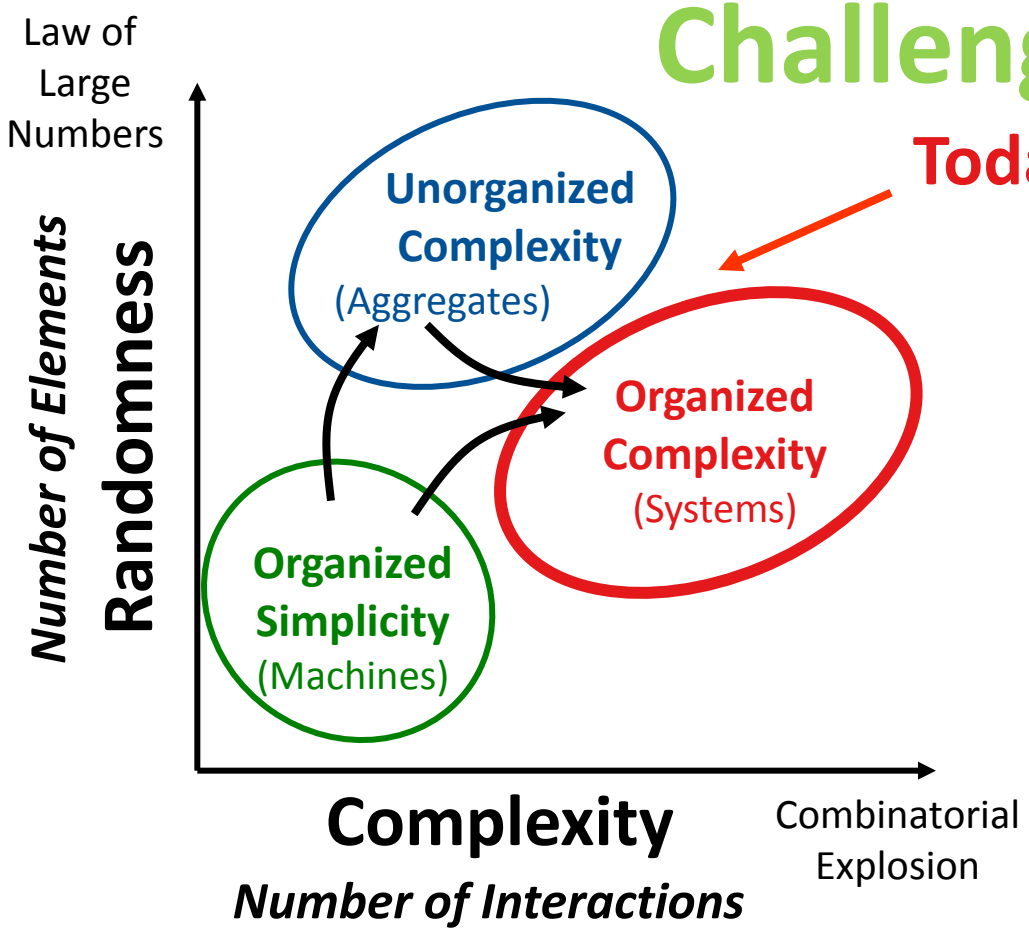

© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

# Why We Have to Look at Risk Differently: Resiliency

- Resiliency = near misses
- Resiliency = heroes
- Resiliency = can't see inside patient
- Resiliency = workarounds common
- Resiliency = hackers

© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

# Organized Complexity: Special Challenges



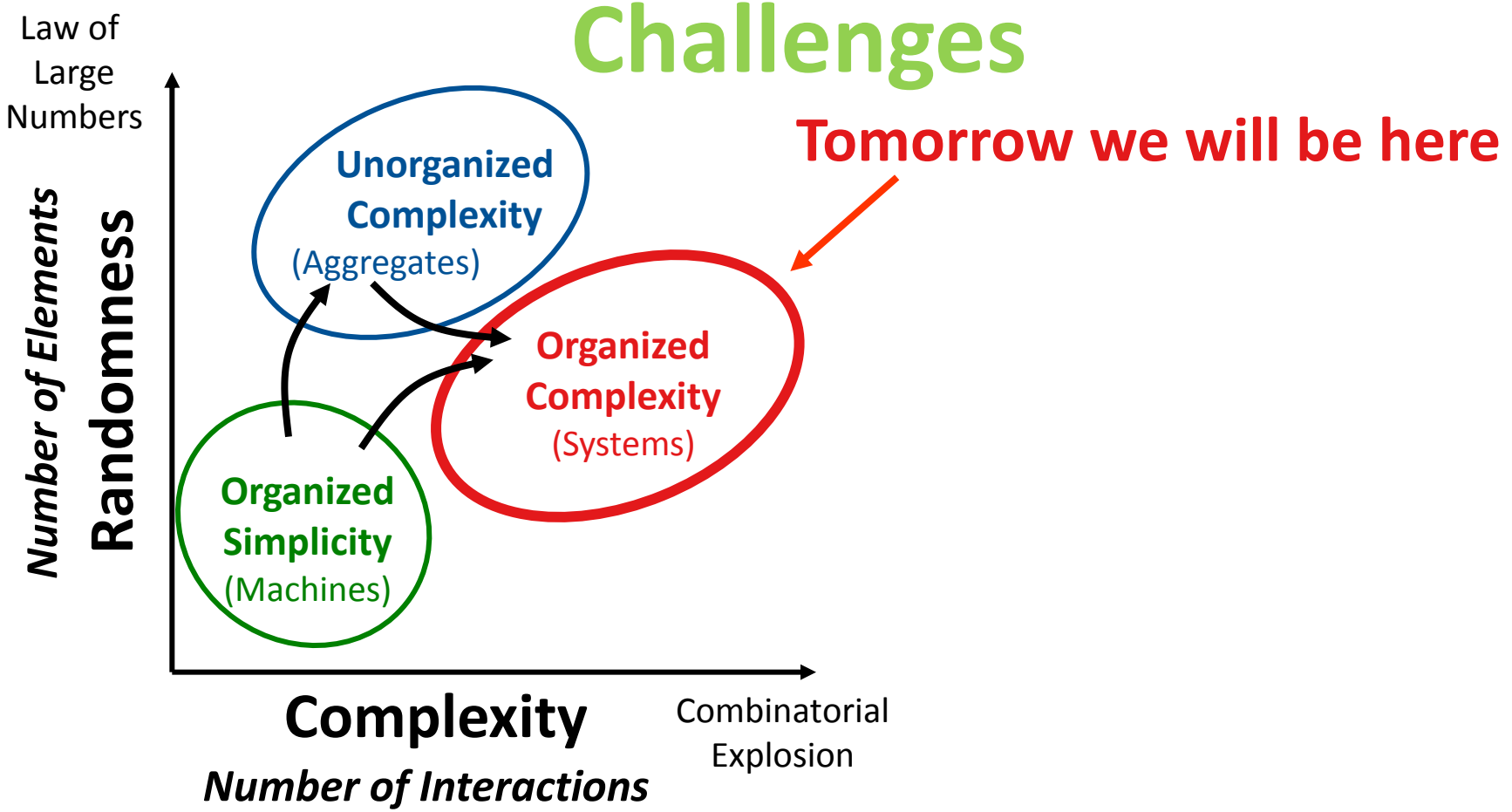

**Today we are here**

- Losses due to interactions amongst components
- Components work fine
- Unmanaged change evolves to an unsafe state over time

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18.

Many thanks to Lane Desborough, Medtronic, for this slide and the thinking behind it.

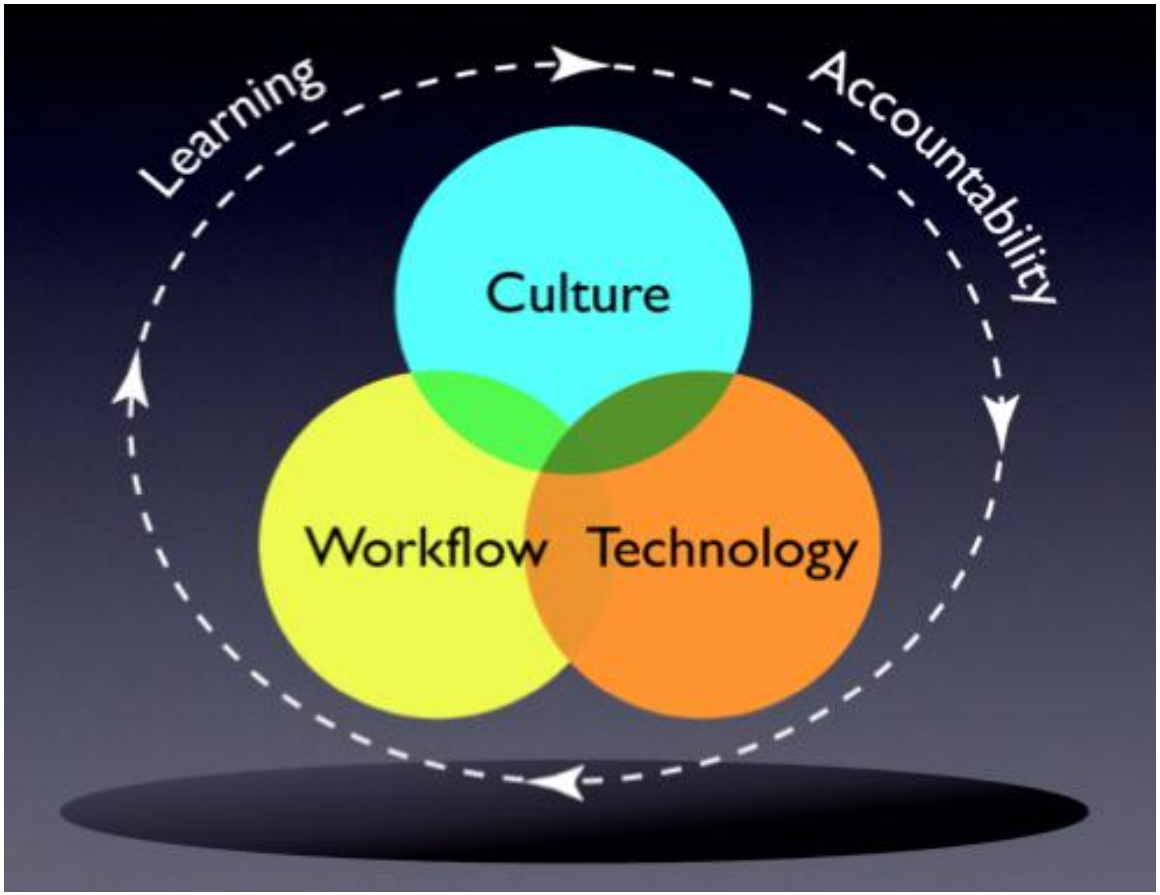
# Organized Complexity: Special Challenges



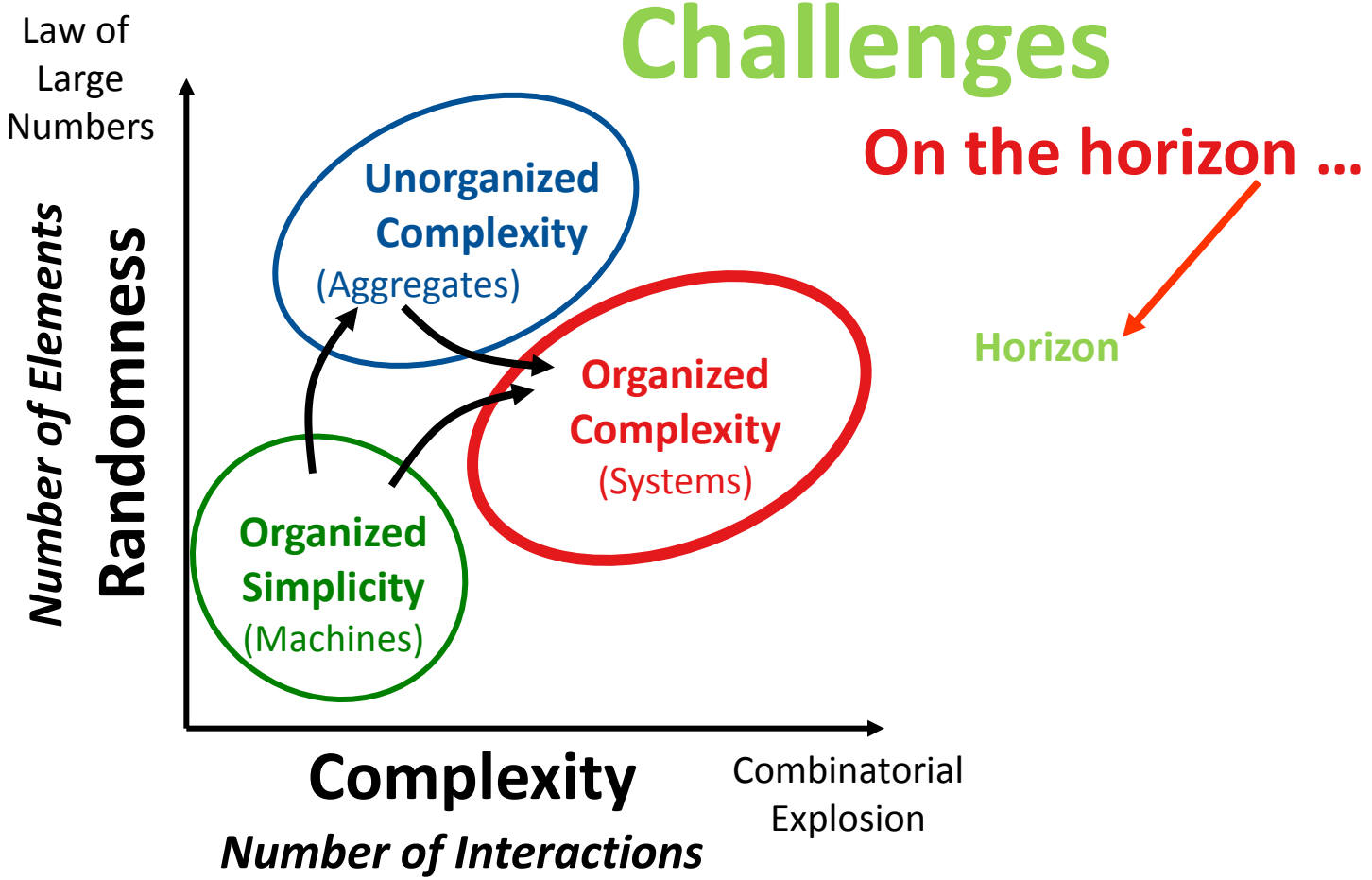

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18.

Many thanks to Lane Desborough, Medtronic, for this slide and the thinking behind it.

# We Won't Be Cyber Safe Until . . .



# Organized Complexity: Special Challenges




From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18.

Many thanks to Lane Desborough, Medtronic, for this slide and the thinking behind it.



amazon.com

Microsoft

Google™

**“The future is already here, it just hasn’t been evenly distributed yet”**

– William Gibson

# Working Together to Achieve Cyber Safety

- Think *System* Safety
- Key: stakeholder engagement
- Build Knowledge
- Can't "Fix:" Healthcare is a complex, socio-technical system
- Not one hospital at a time
- Consensus Standards
- Next Generation Products
- It's Not a Project

© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

# Session IX

# Development of Cybersecurity Tools, Risk Assessments, and Standards for the Healthcare and Public Health Sector

Moderator
Ken Hoyme, MS – Adventium Labs / AAMI

October 22, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Risk Assessment Standards

- NIST SP800-30r1 - Guide for Conducting Risk Assessments
- ANSI/AAMI/ISO 14971, Medical devices -- Application of risk management to medical devices
- ANSI/AAMI/IEC 80001 Family - Application of risk management for IT-networks incorporating medical devices
  - Part 1: Roles, responsibilities and activities
  - Part 2-2: Guidance for the communication of medical device security needs, risks and controls
  - Part 2-8: Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
- AAMI TIR57 - Principles for medical device information security risk management (in development)

# General Security Standards

- NIST SP800-53r4 - Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP800-160 - Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security controls
- ISO/DIS 27799, Health informatics — Information security management in health using ISO/IEC 27002

# Security Standards from the Industrial Controls Domain

- IEC, /TS 62443-1-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.
  - FDA Recognized
- IEC, 62443-2-1 Edition 1.0 2010-11 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
  - Referenced in NIST Framework
  - FDA Recognized
- IEC, /TR 62443-3-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems.
  - FDA Recognized
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
  - Referenced in NIST Framework

# Other relevant security standards and guides

- CLSI AUTO11-A - IT Security of In Vitro Diagnostic Instruments and Software Systems; 2006.
  - FDA Recognized
- ISACA's COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
  - Referenced in NIST Framework
- Council on CyberSecurity (CCS) - The Critical Security Controls for Effective Cyber Defense
  - Referenced in NIST Framework
- HIMSS/NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- HITRUST Common Security Framework (CSF)
  - Integrates NIST, ISO/IEC and other standards and best practices

# Tool Classes

- Risk management
  - Threat modeling
  - Security Risk Assessment models
  - Safety Case tools
- Requirements analysis
- Design/architecture
- Code
  - Static analysis
- Test
  - Robustness Testing
  - Penetration Testing
- In-service operation
  - Audit monitoring
  - Intrusion detection
  - Virus/malware prevention
- Self-assessment
- Frameworks

# Session X

# Building Potential Cybersecurity Solutions/Paths Forward for the Healthcare and Public Health Sector

Moderator

Dale Nordenberg, MD – Medical Device Innovation, Safety and Security Consortium (MDISS)/ Novasano Health & Science

October 22, 2014

Please send questions or comments on this session to: AskMedCyberWorkshop@fda.hhs.gov

# Closing Remarks
# Collaborative Approaches for Medical Device and Healthcare Cybersecurity

October 21-22, 2014
Arlington, VA